Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CA05/000125

International filing date: 03 February 2005 (03.02.2005)

Document type: Certified copy of priority document

Document details:

Country/Office:	US
Number:	60/615,940
Filing date:	06 October 2004 (06.10.2004)

Date of receipt at the International Bureau: 27 April 2005 (27.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PA 1287051

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 25, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/615,940***
FILING DATE: ***October 06, 2004***

PCT/CA05/00125

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

N. Woodson
N. WOODSON
Certifying Officer

PTO/SB/16 (08-03)
Approved for use through 07/31/2008. OMB 0851-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Derek J.	Ritz	Ancaster, Ontario, Canada

□ *Additional inventors are being named on the _____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

SECURITY ARCHITECTURE

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☒ Customer Number 1059

OR

□ Firm or Individual Name					
Address					
Address					
City		State		ZIP	
Country		Telephone		Fax	

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 12
□ CD(s), Number
□ Drawing(s) *Number of Sheets*
□ Other (specify)
☒ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☒ Applicant claims small entity status. See 37 CFR 1.27.
□ A check or money order is enclosed to cover the filing fees
☒ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 022095
□ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($) 80.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.
□ Yes, the name of the U.S. Government agency and the Government contract number are: _____.

[Page 1 of 2]

Respectfully submitted,
SIGNATURE Bhupinder Randhawa
Date October 6 2004
REGISTRATION NO. 47,276
(if appropriate)
TYPED or PRINTED NAME Bhupinder S. Randhawa
Docket Number: 13647-8
TELEPHONE 416-364-7311

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51 The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/17 (10-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2005

Effective 10/01/2004. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($)	80.00

Complete if Known

Application Number	not yet known
Filing Date	filed concurrently herewith
First Named Inventor	RITZ, Derek J.
Examiner Name	N/A
Art Unit	N/A
Attorney Docket No.	13847-8

METHOD OF PAYMENT *(check all that apply)*

□ Check □ Credit card □ Money Order □ Other □ None

☑ Deposit Account:

Deposit Account Number: **022095**

Deposit Account Name: **Bereskin & Parr**

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

□ Charge fee(s) indicated below, except for the filing fee

to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	790	2001	395	Utility filing fee	
1002	350	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	80.00

SUBTOTAL (1) ($) 80.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims		- 20** =		X		=	0.00
Independent Claims		- 3** =		X		=	0.00
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	44	Independent claims in excess of 3
1203	300	2203	150	Multiple dependent claim, if not paid
1204	88	2204	44	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	430	2252	215	Extension for reply within second month	
1253	980	2253	490	Extension for reply within third month	
1254	1,530	2254	765	Extension for reply within fourth month	
1255	2,080	2255	1,040	Extension for reply within fifth month	
1401	340	2401	170	Notice of Appeal	
1402	340	2402	170	Filing a brief in support of an appeal	
1403	300	2403	150	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,370	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	*Recording each patent assignment per property (times number of properties)*	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) ____________

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY			(Complete *(if applicable)*)	
Name (Print/Type)	Bhupinder S. Randhawa	*Registration No. (Attorney/Agent)* 47,276	*Telephone*	(416) 364-7311
Signature	BS Randhawa		*Date*	Octoer 6, 2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRES
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Provisional Patent Application

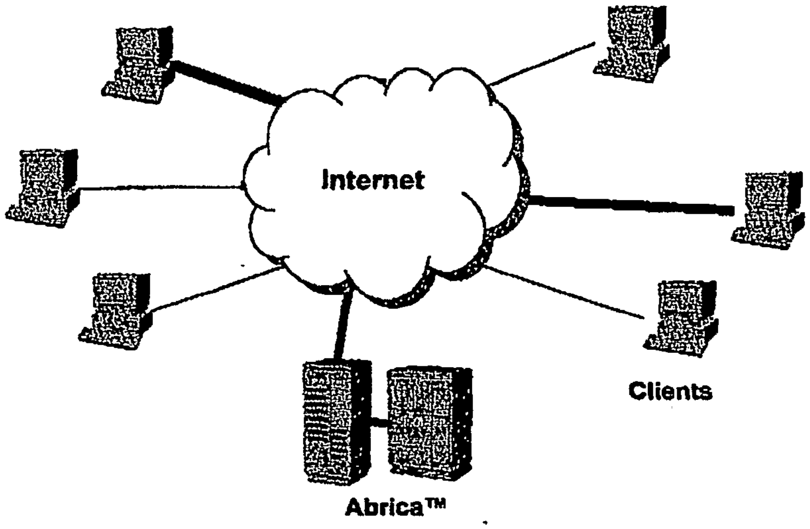
Abrica Security Framework

July 2004

Contents

Abrica™ Security Framework

Overview



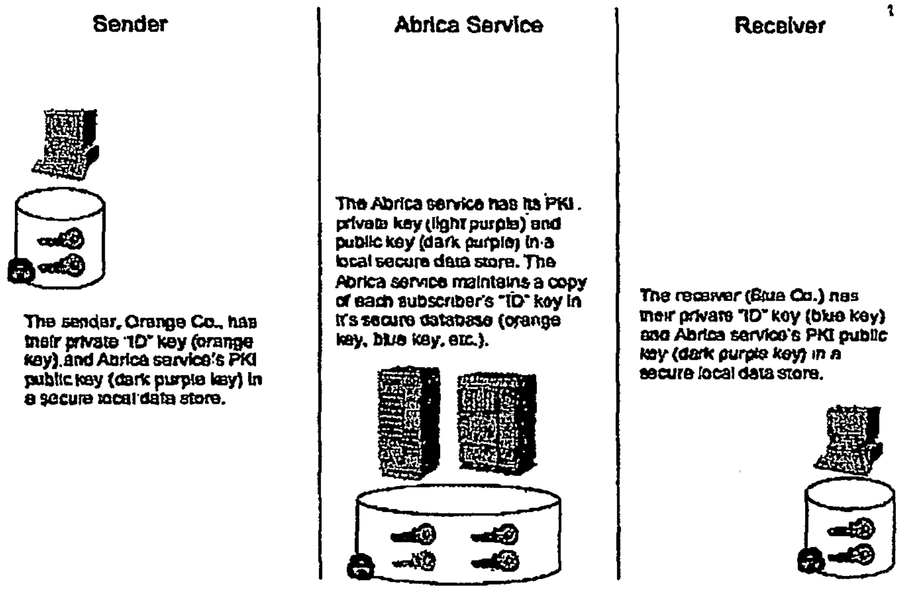
Abrica may be implemented using any technology that allows trading partners and channel partners to communicate with one another and with the Abrica service in electronic form. For example, the different entities may communicate using direct or indirect connections, e-mail, the Internet, a WAN or another type of communication network.

In the present example (shown abovo), the communication mechanism is deployed as an Internet-wide service. Trading partners who subscribe to the Abrica service will use the same core service for sending/receiving transmissions. Abrica will serve as the "forwarder" of transmissions. Each trading partner will post its transmission to the Abrica service where non-repudiation audit trail will be created. From there, the service will forward the transmission to the destination trading partner using email as the conveyance mechanism.

The unique security infrastructure of the Abrica client and server software allows strong encryption and ID-level authentication to be accomplished in a single transmission "round trip" (HTTPS post & status reply). The processes employ cryptographic techniques well-suited to online transaction processing (OLTP) environments supporting large traffic volumes while foregoing the significant overhead and management hurdles associated with systems based purely on public key infrastructure (PKI) technologies.

Key Management

Abrica's key management is illustrated by the graphic below. The Abrica service has an SSL certificate rooted with a recognized certificate authority (CA). Each Abrica subscriber has a copy of the service's public PKI key, plus a unique identifying key (ID key), which was assigned to it by the Abrica service at the time the subscriber joined the network. The Abrica service maintains a copy of each subscriber's ID key along with its own public and private PKI keys.



The sender, Orange Co., has their private "ID" key (orange key), and Abrica service's PKI public key (dark purple key) in a secure local data store.

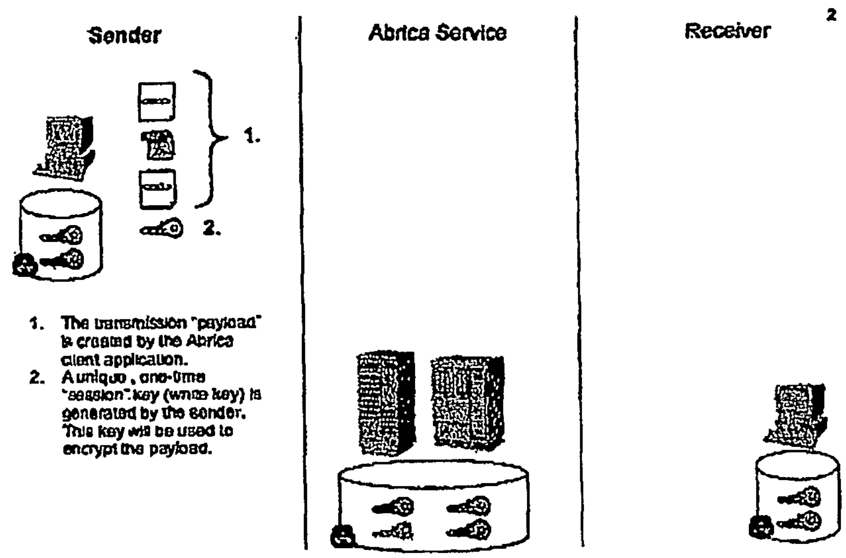
The Abrica service has its PKI private key (light purple) and public key (dark purple) in a local secure data store. The Abrica service maintains a copy of each subscriber's "ID" key in it's secure database (orange key, blue key, etc.).

The receiver (Blue Co.) has their private "ID" key (blue key) and Abrica service's PKI public key (dark purple key) in a secure local data store.

Outbound Transmission to Service

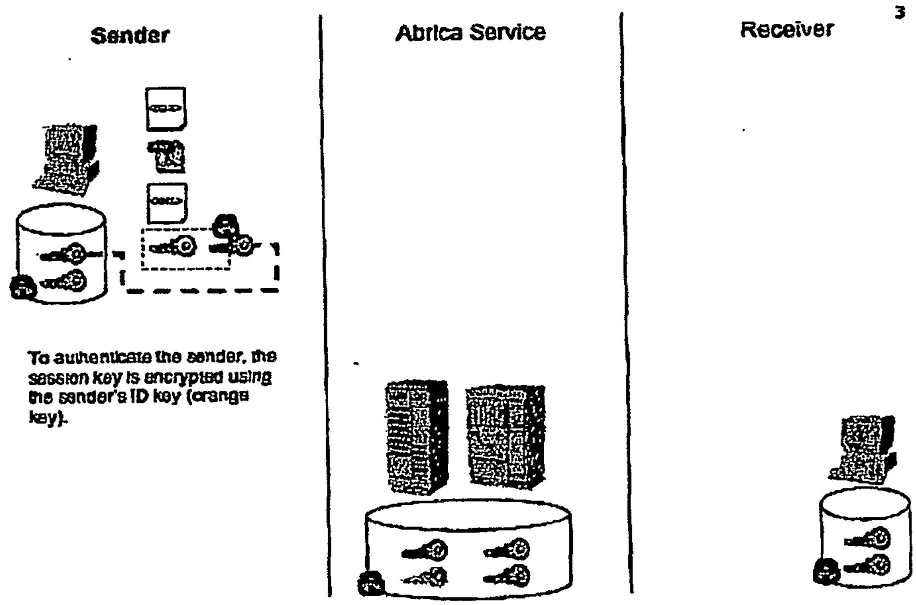
An outbound transmission "payload" is created. It is expected that this payload, which may contain multiple electronic files of various types, will include an indicator that can be used to identify the intended recipient of the transmission.

As a first step, a unique session key is created for each outbound transmission. This session key is a "symmetric key" of appropriate cryptographic strength (e.g. 128 bit).



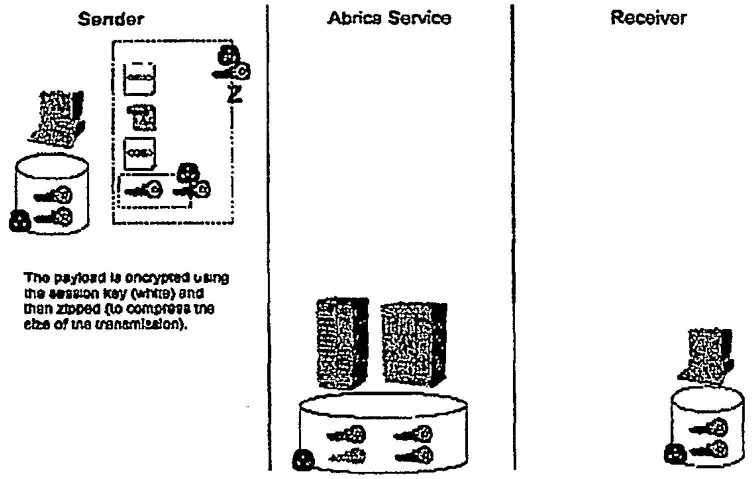
1. The transmission "payload" is created by the Abrica client application.
2. A unique, one-time "session" key (white key) is generated by the sender. This key will be used to encrypt the payload.

As a second step, and in order to authenticate the originator of the transmission, the sender will encrypt a copy of the session key using his unique ID key. This encrypted session key will be included in the transmission payload.



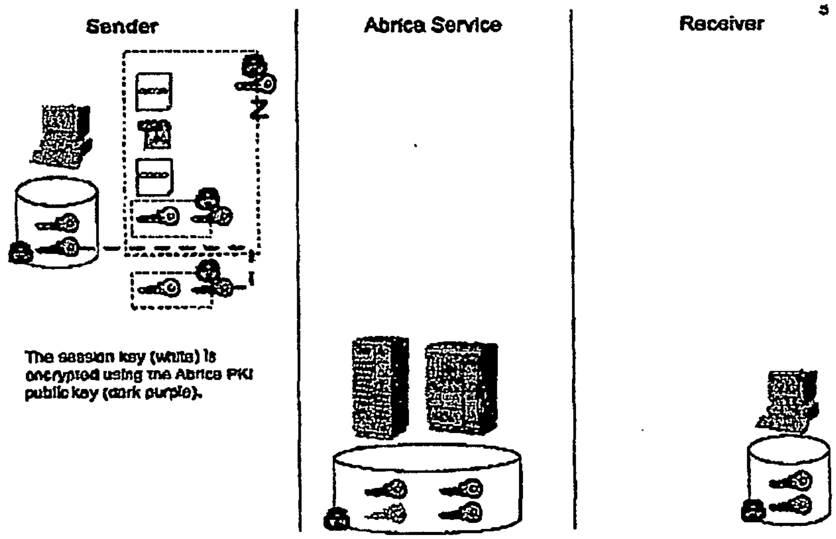
To authenticate the sender, the session key is encrypted using the sender's ID key (orange key).

All Abrica transmissions are sent in an encrypted form. The session key is used to encrypt the transmission payload. Optionally, and to reduce the size of the transmission payload, compression technologies such as ZIP may be employed.



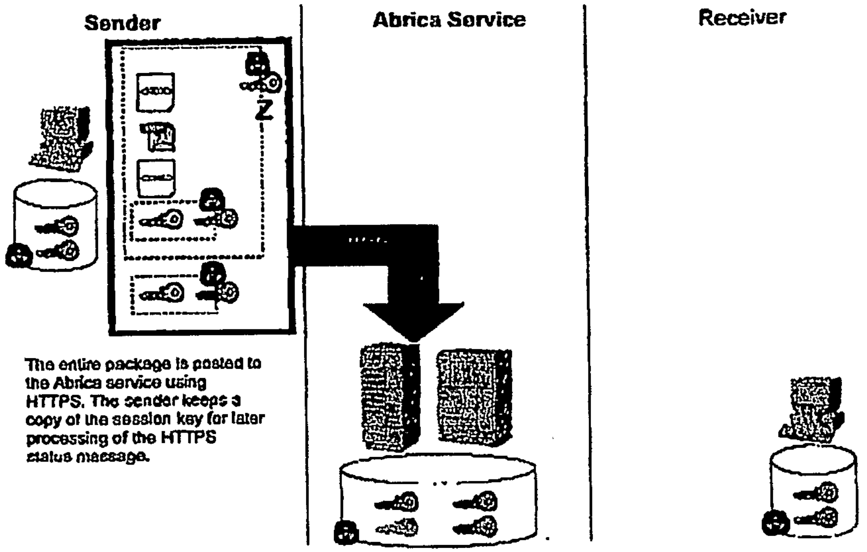
The payload is encrypted using the session key (white) and then zipped (to compress the size of the transmission).

In order to insure that the payload cannot be surreptitiously intercepted (the "man in the middle" attack), the session key is encrypted using the Abrica service's public PKI key. In this way, no entity save the owner of the corresponding PKI private key will be able to obtain the session key needed to decrypt the payload.



The session key (white) is encrypted using the Abrica PKI public key (dark purple).

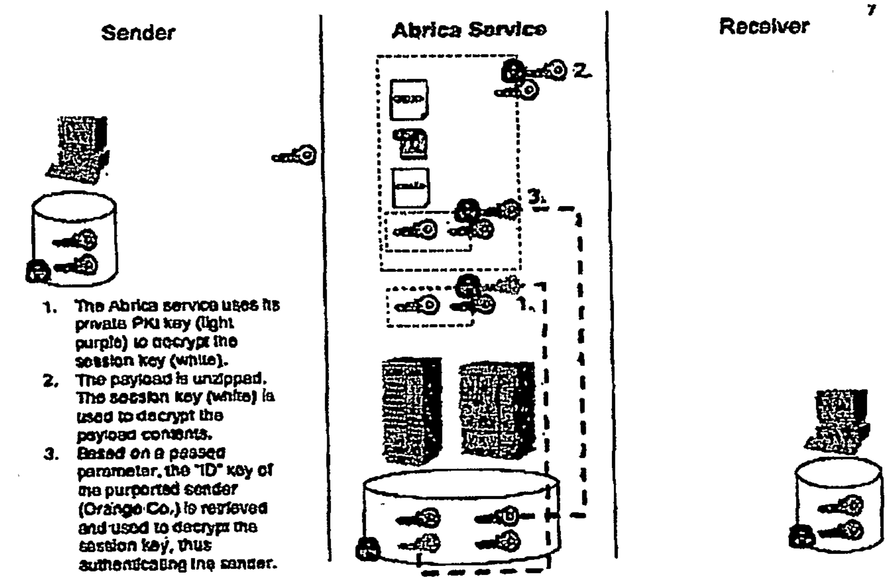
The entire transmission, including the payload, the ID-encrypted session key, and the PKI-encrypted session key, is securely sent to the Abrica service. In the present example, it is posted using HTTPS via a secure socket layer (SSL).



The entire package is posted to the Abrica service using HTTPS. The sender keeps a copy of the session key for later processing of the HTTPS status message.

Processing Inside Service

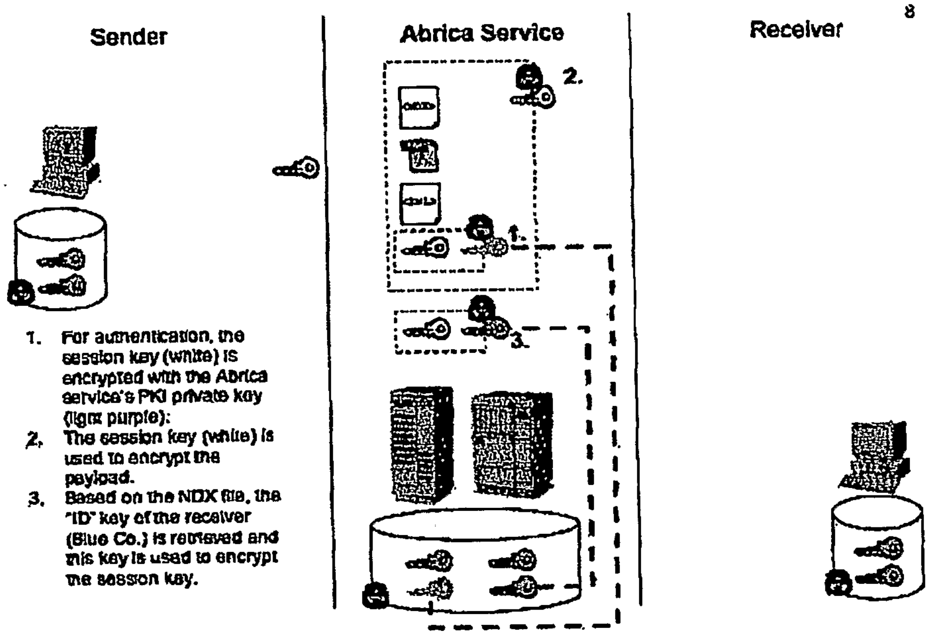
Inbound transmissions received by the Abrica service are processed using a combination of the Abrica PKJ private key and the sender's ID key. In this way, the Abrica service proves itself as the intended recipient (as the sole owner of the necessary private key) and authenticates the purported sender as the true sender (the owner of the corresponding ID key).



1. The Abrica service uses its private PKI key (light purple) to decrypt the session key (white).
2. The payload is unzipped. The session key (white) is used to decrypt the payload contents.
3. Based on a passed parameter, the "ID" key of the purported sender (Orange Co.) is retrieved and used to decrypt the session key, thus authenticating the sender.

After completing internal processing, such as laying down non-repudiation audit trail regarding the sender, the intended receiver, and the payload contents, the Abrica service prepares the transmission for forwarding to the intended recipient. This is done using the Abrica service's private key and the intended recipient's ID key.

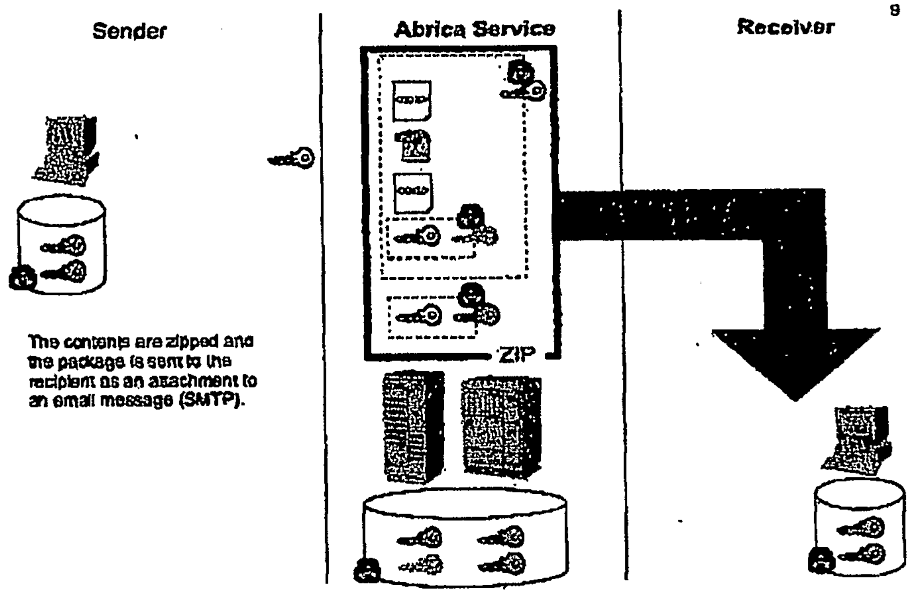
The use of these keys authenticates the Abrica service as the forwarder (again, thwarting a "man in the middle" attack) and insures that only the intended recipient will be able to obtain the session key needed to decrypt the payload.



1. For authentication, the session key (white) is encrypted with the Abrica service's PKI private key (light purple);
2. The session key (white) is used to encrypt the payload.
3. Based on the NDX file, the "ID" key of the receiver (Blue Co.) is retrieved and this key is used to encrypt the session key.

Transmission from Service to Recipient

After processing, the transmission is securely forwarded by the Abrica service to the intended recipient. In the present example, the transmission is sent by simple mail transport protocol (SMTP), essentially arriving in the recipient's email inbox as an email with an encrypted attachment. Optionally, and to reduce the size of the transmission, the payload and the necessary keys may be compressed using ZIP or other appropriate technologies.

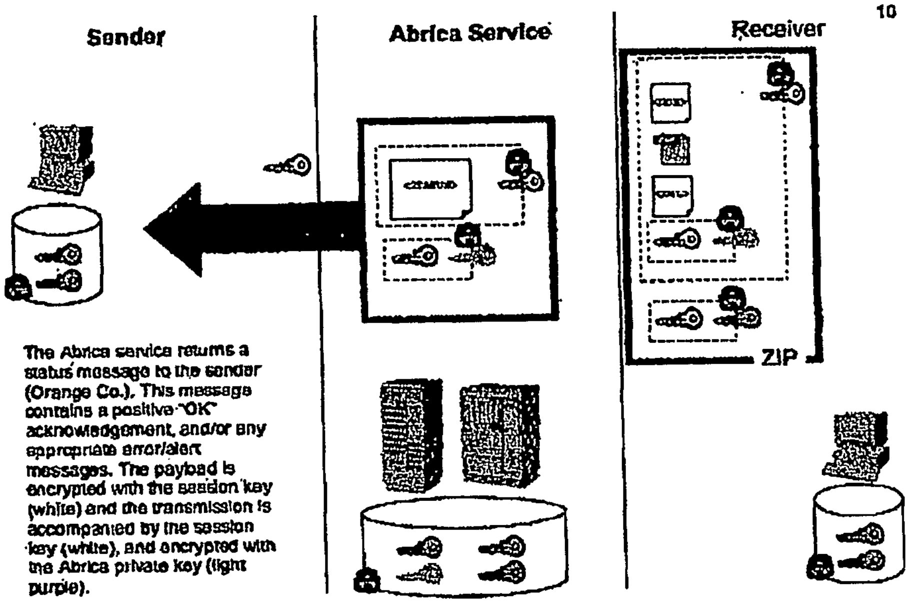


The contents are zipped and the package is sent to the recipient as an attachment to an email message (SMTP).

Status Reply from Service to Sender

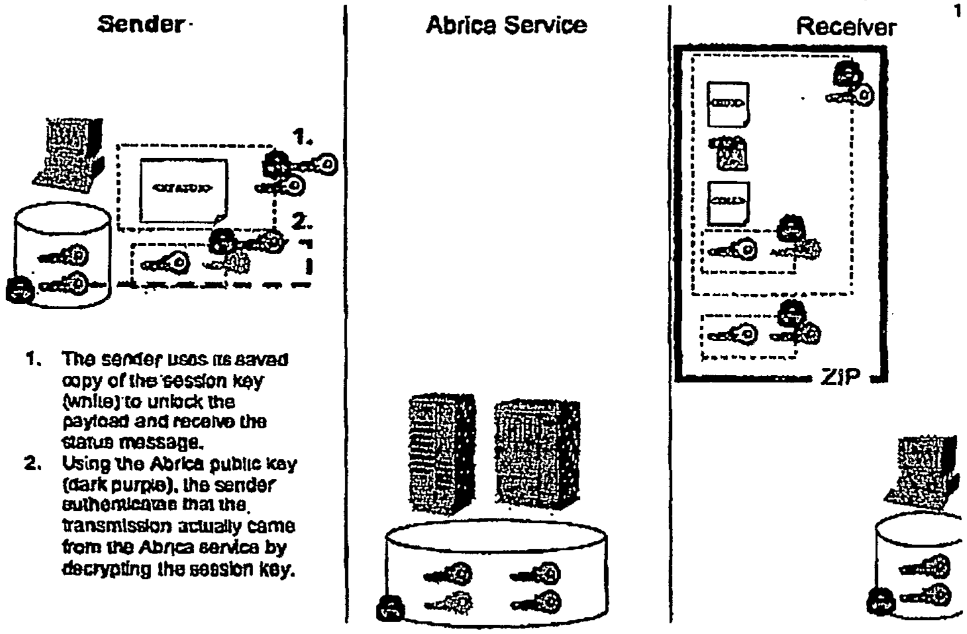
Feedback is provided by the Abrica service to the sender. This feedback provides explicit evidence to the sender that the transmission has been successfully processed and authenticates to the sender that the Abrica service was the recipient of the forwarded transmission.

In the present example, the feedback is provided by the HTTPS return code, which is sent in reply to the original posting. The Abrica services uses its private PKI key to authenticate itself, and the session key to encrypt the transmission.



The Abrica service returns a status message to the sender (Orange Co.). This message contains a positive "OK" acknowledgement, and/or any appropriate error/alert messages. The payload is encrypted with the session key (white) and the transmission is accompanied by the session key (white), and encrypted with the Abrica private key (light purple).

The sender of the transmission receives feedback from the Abrica service, which in the present example is an HTTPS reply. The sender employs the original session key to decrypt the transmission contents and uses the Abrica service's PKI public key to authenticate that the feedback has in fact come from the Abrica service (defeating any attempt at a "man in the middle" attack).

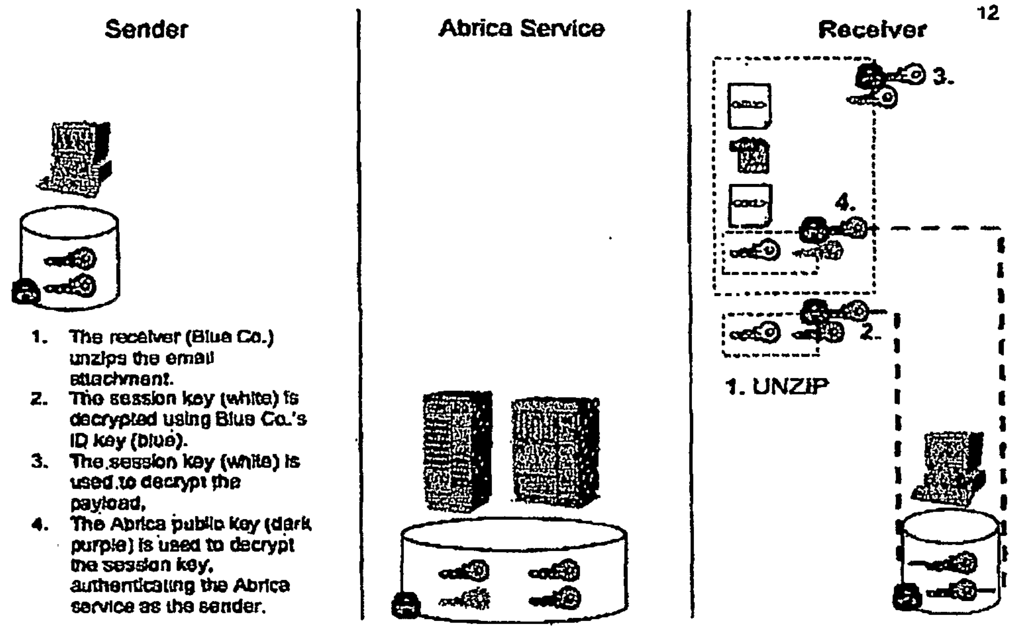


1. The sender uses its saved copy of the session key (white) to unlock the payload and receive the status message.
2. Using the Abrica public key (dark purple), the sender authenticates that the transmission actually came from the Abrica service by decrypting the session key.

Processing by Recipient

The intended recipient receives the sender's original transmission payload via a secure transport mechanism. In the present example, the transmission was received as an encrypted attachment to an email message.

The recipient employs its ID key to decrypt the session key, which can then be used by the recipient to decrypt the sender's original payload. The use of the ID key insures that the intended recipient is the only one who could decrypt the session key (and hence gain access to the encrypted payload). The recipient also employs the Abrica service's public key to authenticate that the transmission has in fact been forwarded to it by the Abrica service. This latter authentication defeats a potential "man in the middle" attack.



1. The receiver (Blue Co.) unzips the email attachment.
2. The session key (white) is decrypted using Blue Co.'s ID key (blue).
3. The session key (white) is used to decrypt the payload.
4. The Abrica public key (dark purple) is used to decrypt the session key, authenticating the Abrica service as the sender.

Patent Application Data Sheet

Application Information

Application Type::	Provisional
Subject Matter::	Utility
Title::	SECURITY ARCHITECTURE
Attorney Docket Number::	13847-8
Small Entity?::	Yes

Applicant Information

Inventor Authority Type::	Inventor
Primary Citizenship Country::	Canada
Status::	Full Capacity
Given Name::	Derek
Middle Name::	J.
Family Name::	Ritz
Name Suffix::	
City of Residence::	Ancaster
State or Prov. Of Residence::	Ontario
Country of Residence::	Canada
Street of mailing address::	157 Amberly Blvd.
City of mailing address::	Ancaster
State or Province of	

mailing address::	Ontario
Country of mailing address::	Canada
Postal or Zip Code of mailing address::	L9G 3V3

Correspondence Information

Correspondence Customer Number::	001059
Phone Number::	416-364-7311
Fax Number::	(416) 361-1398
E-Mail Address::	brandhawa@bereskinparr.com

Representative Information

Representative Customer Number::	001059